

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-171517

(43)公開日 平成8年(1996)7月2日

(51)Int.Cl.⁸

G 0 6 F 12/14
G 0 6 K 17/00
19/073

識別記号 庁内整理番号

3 1 0 A
T

F I

技術表示箇所

G 0 6 K 19/ 00

P

審査請求 未請求 請求項の数2 FD (全5頁)

(21)出願番号

特願平6-333819

(22)出願日

平成6年(1994)12月19日

(71)出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(72)発明者 稲田 真弓

東京都新宿区市谷加賀町一丁目1番1号

大日本印刷株式会社内

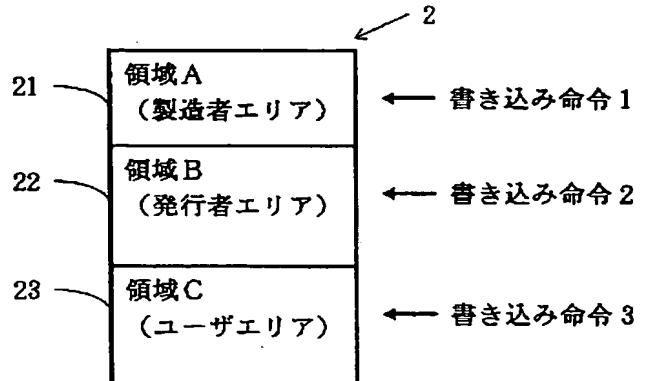
(74)代理人 弁理士 小西 淳美

(54)【発明の名称】 情報記憶媒体

(57)【要約】

【目的】 カード等の情報記憶媒体の改ざんや偽造防止を困難にする。

【構成】 書き換え可能な情報記憶用メモリを複数の領域に分割して使用する情報記憶媒体について、分割された領域毎に、書き込み命令や読み出し命令等の書き換え命令が異なるようとする。また、分割された領域毎に使用可能な書き換え命令を1以上の分割領域で複数使用できるようにする。



【特許請求の範囲】

【請求項 1】 書き換え可能な情報記憶用メモリを複数の領域に分割して使用する情報記憶媒体において、各分割された領域毎に書き換え命令が異なることを特徴とする情報記憶媒体。

【請求項 2】 分割された領域毎に使用可能な書き換え命令が、1以上の分割領域で複数あることを特徴とする請求項1記載の情報記憶媒体。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、ICカード等の外部からの命令によって、その内部データを書き換えることが可能な情報記憶媒体に関し、特に、改ざん、偽造防止等のセキュリティ対策に有効な情報記憶媒体に関する。

【0002】

【従来の技術】 近年、磁気カード等の他にも、ICメモリーや光メモリー等の大量の情報を記憶できる情報記憶手段を有し、且つ外部からの命令によって保有する記憶データの書き換え等を処理するICカード等が普及が始まっている。そして、通常、ICカード等の情報記憶媒体は、そのメモリを、カード製造者が扱う「カード製造者領域」、カード発行者が扱う「カード発行者領域」、サービス提供者が扱う「ユーザ領域」等と複数の領域に分割して使用している。そして、カード発行処理の際は、これら領域に所定の初期データを書き込んだ後、カード所有者に渡され利用されることとなる。

【0003】 なお、カード発行者とは、例えば、或る技術形式のカードを販売している会社である。そして、例えば百貨店等のサービス提供者が自社用の顧客カードとして、所定の初期データを書き込んだ顧客カードを顧客に渡して、顧客はカード所有者となる。カード所有者は、サービス提供者が備えたユーザアプリケーションシステムのカード利用端末を用いてカードを利用すると、ユーザ領域の記憶情報が書き換えられたり、新たに情報が追加されることになる。ところで、或るカード発行者の或る一つの技術形式のカードでもサービス提供者が異なれば、サービス提供者に関係する部分のメモリ内容は当然異なるので、その部分はサービス提供者がその部分の初期データを書き込む。また、或る一つのカード発行者のカードでも技術形式が異なれば、それに該当する部分が異なるので、カード発行者が初期データを書き込む。しかし、カード発行者がサービス提供者に渡すカードについて、カード発行者が書き込むべき初期データを全て書き込んでもよいが、原始レベルの初期データ等はカード製造者に書き込みを依頼することもある。従って、カード製造者は依頼された内容を書き込むことになるが、製造管理上等の種々の理由でカード製造者独自の形式で製造ロット番号等の所定の情報を書き込む。以上のようにして、カード発行処理は、カード製造者→カード発行者→サービス提供者という、流れで行われることがある。

る。

【0004】 また、セキュリティ対策の為に、カード製造者からカード発行者へ、カード発行者からサービス提供者へと、カードが渡される各過程で、それぞれ正しい発行者、正しいサービス提供者であることを、暗号化した照合キーを記憶させて照合キーの照合によって行うこともある。

【0005】

【発明が解決しようとする課題】 しかし、万が一、キー情報や書き換え命令に関する命令コードが盗み出されてしまうと、データの書き換えを不正に行う、データの改ざん行為が行われる恐れがある。また、カード発行の際に書込んだデータ等も読み出すことが出来ると、それらのデータを用いて別のカードを偽造される恐れもあるという問題があった。そこで、本発明の目的は以上のような問題点を解決し、記憶されているデータの改ざんや、記憶されているデータを読み出して情報記憶媒体を偽造することができない、セキュリティ性の高い情報記憶媒体を提供することである。

【0006】

【課題を解決するための手段】 そこで、上記課題を解決するために、本発明の情報記憶媒体は、分割したメモリの領域毎に書き込み命令や読み出し命令である書き換え命令を変えるようにしたものである。

【0007】 すなわち、請求項1の情報記憶媒体は、書き換え可能な情報記憶用メモリを複数の領域に分割して使用する情報記憶媒体において、各分割された領域毎に書き換え命令が異なるものとする。

【0008】 また、請求項2の情報記憶媒体は、上記請求項1の情報記憶媒体において、分割された領域毎に使用可能な書き換え命令が、1以上の分割領域で複数あるようにしたものである。

【0009】

【作用】 請求項1の情報記憶媒体では、領域毎に書き換え命令が異なるので、或る領域に関する書き換え命令が盗まれたとしても、他の領域の書き換え命令が不明であるので、情報記憶媒体全体の記憶データの書き換えを必要とする偽造は不可能である。

【0010】 請求項2の情報記憶媒体では、書き換えに照合キーを使用する場合等にも対処できるものである。すなわち、或る一つの領域に複数の書き換え命令が使用できるために、それを逆に命令基準でみれば、例えば、複数の領域にまたがって部分的に重複して同一の書き換え命令を使用可能とすることができる（但し、分割メモリ領域の全てに共通の書き換え命令は無い）。従って、メモリ領域をまたがって照合キーを設定して、メモリ領域毎に取り扱う者の正当性をチェックすることも可能となり、よりセキュリティ性が高められる。

【0011】

【実施例】 以下、本発明の情報記憶媒体について、その

実施例を図1及び図2を参照しながら、さらに詳述する。

【0012】なお、本発明の情報記憶媒体のハードウェア構成は、従来公知のICカード等の外部からの命令によって内部の記憶情報を書き換えることができる、情報記憶媒体と同様でよい。すなわち、図3は本発明の情報記憶媒体のブロック図であり、情報記憶媒体1は、少なくとも、ICメモリ等の情報記憶手段2と、情報記憶手段2と、利用端末等に内蔵されたリーダライタ装置Aとの間に介在し、リーダライタ装置から与えられた命令に従い、記憶されたデータの書き換え等をする、CPU等の情報制御手段3と、から構成される。

【0013】なお、本明細書中での「書き換え命令」とは、少なくとも、データの書き込み命令のことである。書き込み命令の乱用が防止されれば、書き換えは不可能だからである。しかし、既存の記憶データを参照したり、記憶データの在り処を探したりすることで緻密に行う手口に対処するには、データの読み出し命令に対しても書き込み命令と同様に、メモリ領域で変えた方が良い。従って、データの読み出し命令は全領域で共通であってもよいが、各領域で異なっていた方がよい。ただし、読み出し命令については、要求されるセキュリティレベルや、対象とする情報記憶媒体を使用するシステム側の機能との関係で適宜決めればよい。

【0014】先ず、本発明の情報記憶媒体について、各メモリ領域毎に書き換え命令が異なる請求項1の発明の一実施例を説明する。

【0015】図1に、本発明の情報記憶媒体の特徴的な部分である、データ書き換え命令と分割メモリとの対応関係の一例を示す。同図では、情報記憶媒体が備える情報記憶手段としてのメモリ2は、21で示す製造者エリアとなる領域Aと、22で示す発行者エリアとなる領域Bと、23で示すユーザエリアとなる領域Cと、に三分割されている。そして、本実施例は、書き換え命令として書き込み命令を各領域で変えて、各領域毎に一つの書き込み命令を対応させた例である。すなわち、各領域に対する書き込み命令は、領域Aに対しては書き込み命令1のみが有効であり、領域Bに対しては書き込み命令2のみが有効であり、領域Cに対しては書き込み命令3のみが有効である状態を同図は示している。

【0016】そして、カード発行処理の最初のステップは、カード製造者において領域Aの部分に、例えば、カード発行日、カード製造ロット番号等のカード発行処理に必要な所望のデータ等を、書き込み命令1により書き込む。次いで、領域Aへの発行処理が完了したカードは、カード製造者からカード発行者に渡される。

【0017】そして、カード発行者において領域Bの部分に例えば、使用するファイルのディレクトリ情報等の領域Cの使用の際に基本的に必要な情報等を、書き込み命令2により書き込む。次いで、領域A及び領域Bへの發

行処理が完了したカードは、カード発行者からサービス提供者に渡される。

【0018】そして、サービス提供者において領域Cの部分に例えばカード所有者の氏名、ID番号等の一枚ずつのカードで異なるデータや共通のデータ等を、書き込み命令3により書き込む。

【0019】以上の一連の発行処理操作によって、カードはカード所有者が利用可能な状態となる。

【0020】上述した発行処理操作においては、セキュリティ性は次のように確保される。すなわち、カード製造者は領域A（製造者エリア）に書き込み命令1を使用して初期データの書き込みを行う。但し、書き込み命令1は、領域Aのみにだけ有効であるために、他の領域、すなわち領域Bと領域Cに対して書き込みを行うことは出来ない。従って、仮に、カード製造者が領域Aの書き込み命令1を誤って外部に盗まれてしまったとしても、領域Bと領域Cの書き込み命令は異なっているために、それらの領域に対しては書き込み命令1は使用できず、盗んだ命令を用いて他のカードを偽造することは困難である。また、仮にカード製造者が書き込み命令1の他にさらに発行処理中のカードも盗まれてしまったとしても、領域Bと領域Cに対する書き込み命令は異なっているために、盗んだカードに対して、たとえ領域Aの内容が都合よく書き換えられても、領域Bと領域Cに対しては書き込み命令1は使用できず、カードの改ざんは困難である。

【0021】以上は、カード製造者が担う領域Aへの発行処理に対するセキュリティ性を述べたものであるが、他の領域に対する発行処理を担うカード発行者、サービス提供者においても、同様なことが言える。

【0022】このように、本発明の情報記憶媒体では、全メモリ領域に対して書き込みを行うには複数の命令を使い分ける必要がある。しかも、上述した発行処理では、発行処理の各ステップを担当する者が自身の処理に関する書き込み命令のみを保有して使えばよいので、他領域の命令は保有しないようにすることができる。その結果、カードの全メモリ領域に対する複数の命令を空間的、時間的に分けて保有し使用することができる。発行処理の一ステップを担う或者者から命令が盗まれても、カード全体に対する書き込みまでは行えず、カード全体に対する偽造や改ざんは困難である。

【0023】また、以上のように各メモリ領域毎に書き換え命令を変えておけば、発行処理を行う際に、例えば、メモリ領域Aへの発行処理ならば、メモリ領域B及びメモリ領域Cと、不必要領域にデータを書き込んでしまうというトラブルも未然に防ぐこともできる。

【0024】次に、本発明の情報記憶媒体について、分割されたメモリ領域について複数、（ここでは二種類）の書き換え命令が対応する請求項2の発明の一実施例を説明する。

【0025】図2は当実施例による情報記憶媒体の、分割されたメモリ領域とデータ書き換え命令との対応関係を示す。同図でも、図1に例示した場合と同様に、情報記憶媒体が備える情報記憶手段としてのメモリ2は、21で示す製造者エリアとなる領域Aと、22で示す発行者エリアとなる領域Bと、23で示すユーザエリアとなる領域Cと、に三分割されている。そして、本実施例では、書き換え命令として書き込み命令を各領域で変えて、一部のメモリ領域に対して複数の書き込み命令が有効であり、且つ一つの書き換え命令が全ての分割されたメモリ領域に対応しない様にしつつ、一つの書き換え命令が複数の領域に有効であるようにした例である。すなわち、図2は、各領域に対する書き込み命令は、領域Aに対しては書き込み命令1のみの一種類のみが有効であり、領域Bに対しては書き込み命令1と書き込み命令2の二種類のみが有効であり、領域Cに対しては書き込み命令2と書き込み命令3の二種類のみが有効である状態を示している。また、当実施例の場合の情報記憶媒体では、照合キーを参照しないと書き換えないようになっており、領域Bで使用する照合キーBは領域Bに、領域Cで使用する照合キーCは領域Cに書き込まれている。

【0026】そして、先の実施例と同様に、カード製造の最初の工程である、カード発行処理はカード製造者において領域Aの部分に例えば、カード発行日、カード製造ロット番号等のカード発行処理に必要な所望のデータ等を、書き込み命令1により書き込む。また、この書き込み命令1は、メモリ領域Bに対しても有効であり、これにてメモリ領域Bに照合キーBを書き込む。次いで、領域B内の照合キーを含む領域Aの発行処理が完了したカードは、カード製造者からカード発行者に渡される。

【0027】そして、カード発行者において領域Bの部分に例えば、使用的ファイルのディレクトリ情報等の領域Cの使用の際に基本的に必要な情報等を、書き込み命令2により書き込む。この際の書き込み処理は、それに先立ち領域Bに格納されている照合キーBを読みだして、発行者が保有している期待値と比較検証して、キーを照合して一致すれば書き込み命令2が実行できるようになっている。このようにして、正当なカード処理資格を有する者か否かがカード側からチェックされる。また、書き込み命令2はメモリ領域Cに対しても有効であり、これにてカード発行者はメモリ領域Cに、さらに第2の照合キーCを書き込む。また、先に照合した照合キーBを照合キーB'に書き換えて、照合キーBを再使用できなくなる（カード発行処理は一回で良いため、偽造、改ざんにつながる照合キーの複数回使用を予防する意味がある）。なお、照合キーは、暗号化されてなくてもよいが、暗号化しておく方が望ましい。次いで、領域B及び領域C内の照合キーを含む領域A及び領域Bの発行処理が完了したカードは、カード発行者からサービス

提供者に渡される。

【0028】そして、サービス提供者において領域Cの部分に例えばカード所有者の氏名、ID番号等の一枚ずつのカードで異なるデータや共通のデータ等を、書き込み命令3により書込む。この際、上記カード発行者の場合と同様に、照合キーCの照合により書き換え処理を行う者がチェックされた上で、書き込み処理は実行される。

【0029】以上の一連の発行処理操作によって、カードはカード所有者が利用可能な状態となる。

【0030】上記の発行処理操作においては、セキュリティ性は次のように確保される。すなわち、カード製造者が使用する書き込み命令1は、領域Aと領域Bだけに有効であるため、領域Cに書き込みを行うことは出来ない。従って、仮に、カード製造者が領域Aの書き込み命令1を誤って外部に盗まれてしまったとしても、書き込み命令1は領域Cに対しては有効でない上、領域Cに対しては照合キーを知らなければ書き込めず、盗んだ命令を使用して他のカードを偽造することは困難である。また、仮にカード製造者が書き込み命令1の他にさらに発行処理中のカードも盗まれてしまったとしても、領域Cへの書き込みまでは出来ず、同様に偽造はカードの改ざんは不可能である。

【0031】同様に、カード発行者が使用する書き込み命令2は、領域Bと領域Cとに有効であり、領域Aに書き込みを行うことはできない。その上、領域Bについても、照合キーBの照合に成功しなければ、書き込み命令2自身も無効であり、しかも、書き込み済のカードでは変更後の照合キーB'の照合に成功しなければ命令は実行できない。従って、書き込み命令2や照合キーBを誤って外部に盗まれてしまったとしても、市場で流通利用されている初期設定完了済のカードに対して、領域Aの書き込み命令は異なっている為に使用できず、領域B及び領域Cについても照合キーB'が漏洩しなければ安全である。

【0032】以上のこととは、サービス提供者が使用する書き込み命令3及び照合キーCについても同様に言える。

【0033】上記の実施例では、分割された或る一つのメモリ領域に対して複数の書き換え命令が対応している。従って、セキュリティ対策に照合キーを使用する場合に対しても、対応が可能で、前記した一分割メモリー書き換え命令の形式の実施例が有するセキュリティ性に加えて、さらに高度のセキュリティ性を確保できる。

【0034】また、発行処理を行う際に、例えば、メモリ領域Aへの発行処理ならば、メモリ領域Cへの不必要データの書き込みを、メモリ領域Bへの発行処理ならば、メモリ領域Aへの不必要データの書き込みを、と不必要領域へデータを書き込んでしまうというトラブルも未然に防ぐこともできる。

【0035】

【発明の効果】請求項1の本発明の情報記憶媒体によれば、全メモリ領域に対して書き込みを行うには複数の書き込み命令が必要である。従って、発行処理の一ステップを担う者から一つ命令が盗まれても、カード全体に対する書き込みまでは行えず、偽造や改ざんを防止できる。また、カードがカード所有者に渡り市場に流通し使用されている状況でも、カード所有者が利用するカード利用端末から書き換え命令が盗まれても、その書き換え命令では一部のメモリ領域しか対応できない様にすることができるるので、カードの偽造や改ざんを防止できる。

【0036】また、請求項2の本発明の情報記憶媒体によれば、分割されたメモリ領域に対して複数の書き換え命令が使用できる様にしてあるので、カード製造者、カード発行者、サービス提供者等とカードを扱うステップやレベルに応じて、使用する書き換え命令を変えて、且つそれらの間で照合キーを用いて、扱う者の正当性をチ

エックするセキュリティ方法においても、より安全にカード偽造や改ざんを防止できる。

【図面の簡単な説明】

【図1】本発明の情報記憶媒体の一実施例による、メモリ分割と書き換え命令との対応関係の説明図。

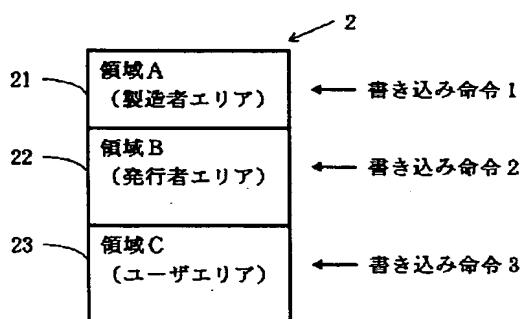
【図2】本発明の情報記憶媒体の他の実施例による、メモリ分割と書き換え命令との対応関係の説明図。

【図3】本発明の情報記憶媒体の一実施例の構成を示すブロック。

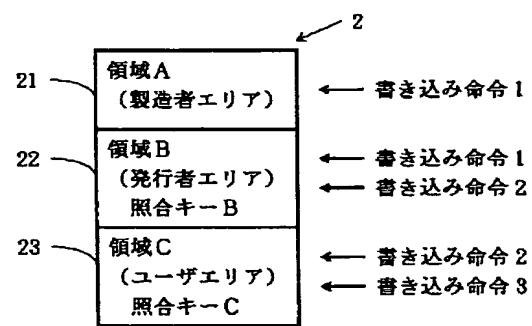
【符号の説明】

- 1 情報記憶媒体
- 2 情報記憶手段、メモリ
- 21 領域A：製造者エリア
- 22 領域B：発行者エリア
- 23 領域C：ユーザエリア
- 3 情報制御手段
- A リーダライタ装置

【図1】



【図2】



【図3】

